command line settings, loading into program processes, and window hooks (these settings are disabled by default).

3.2.4. Configuring update settings

Your computer's security depends directly on updating the threat signatures and program modules regularly. In this window, the Setup Wizard asks you to select a mode for program updates, and to configure a schedule.

- Automatically. Kaspersky Internet Security checks the update source for update packages at specified intervals. Scans can be set to be more frequent during virus outbreaks and less so when they are over. When the program detects fresh updates, it downloads them and installs them on the computer.
- Every 1 day(s).Updates will run automatically according to the schedule created. You can configure the schedule by clicking Change.
- Manually. If you choose this option, you will run program updates yourself.

Note that the threat signatures and program modules included with the software may be outdated by the time you install the program. That is why we recommend downloading the latest program updates. To do so, click Update now. Then Kaspersky Internet Security will download the necessary updates from the update servers and will install them on your computer.

If you want to configure updates (set up network properties, select the resource from which updates will be downloaded, or select the update server located nearest to you), click Settings.

3.2.5. Configuring a virus scan schedule

Scanning selected areas of your computer for malicious objects is one of the key steps in protecting your computer.

When you install Kaspersky Internet Security, three default virus scan tasks are created. In this window, the Settings Master asks you to choose a scan task setting:

Scan startup objects

Kaspersky Internet Security scans startup objects automatically when it is started by default . You can edit the schedule settings in another window by clicking Change.

Scan critical areas

Interactive. This mode provides more customized defense of your computer's data than Basic mode. It can trace attempts to alter system settings and suspicious activity in the system.

All of the activities listed above could be signs of malicious programs or standard activity for some of the programs you use on your computer. You will have to decide for each separate case whether those activities should be allowed or blocked.

If you choose this mode, specify when it should be used:

- **Enable Registry Guard** – ask for user decision if attempts to alter system registry keys are detected.

  If the application is installed on a computer running Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, or Microsoft Windows Vista x64, the interactive mode settings listed below will not be available.

- **Enable Application Integrity Control** – prompt user to confirm actions taken when modules are loaded into applications being monitored.
- **Enable Extended Proactive Defense** – enable analysis of all suspicious activity in the system, including opening browser with command line settings, loading into program processes, and window hooks (these settings are disabled by default).

3.2.4. Configuring update settings

Your computer's security depends directly on updating the threat signatures and program modules regularly. In this window, the Setup Wizard asks you to select a mode for program updates, and to configure a schedule.

- **Automatically**. Kaspersky Anti-Virus checks the update source for update packages at specified intervals. Scans can be set to be more frequent during virus outbreaks and less so when they are over. When the program detects fresh updates, it downloads them and installs them on the computer. This is the default setting.
- **Every 1 day(s)**.Updates will run automatically according to the schedule created. You can configure the schedule by clicking **Change**.
- **Manually**. If you choose this option, you will run program updates yourself.

Note that the threat signatures and program modules included with the software may be outdated by the time you install the program. That is why we recommend downloading the latest program updates. To do so, click **Update now**. Then Kaspersky Anti-Virus will download the necessary updates from the update servers and will install them on your computer.

If you want to configure updates (set up network properties, select the resource from which updates will be downloaded, or select the update server located nearest to you), click **Settings**.

3.2.5. Configuring a virus scan schedule

Scanning selected areas of your computer for malicious objects is one of the key steps in protecting your computer.

When you install Kaspersky Anti-Virus, three default virus scan tasks are created. In this window, the Settings Master asks you to choose a scan task setting:

Scan startup objects

Kaspersky Anti-Virus scans startup objects automatically when it is started by default. You can edit the schedule settings in another window by clicking **Change**.

Scan critical areas

To automatically scan critical areas of your computer (system memory, Startup objects, boot sectors, Windows system folders) for viruses, check the appropriate box. You can configure the schedule by clicking **Change**.

The default setting for this automatic scan is disabled.

Full computer scan

For a full virus scan of your computer to run automatically, check the appropriate box. You can configure the schedule by clicking **Change**.

The default setting, for scheduled running of this task, is disabled. However, we recommend running a full virus scan of your computer immediately after installing the program.

3.2.6. Restricting program access

Since several people with different levels of computer literacy might use a personal computer, and since malicious programs can disable protection, you are given the option of password-protecting access to Kaspersky Anti-Virus. Using a password can protect the program from unauthorized attempts to disable protecting or change settings.

To enable password protection, check **Enable password protection** and complete the **Password** and **Confirm password** fields.